EXHIBIT "1"

December 28th 2023

To: Wood County Board of Elections (BOE): Julie Baumgardner (Director); Terry L Burton (Director); Jonathan R Jakubowski (Board Member); John T. Cuckler (Board Member); Andrew J. Newlove (Board Member); Mike Zickar (Board Member)

CC: Honorable Teresa Gavarone (Senator); Honorable Haraz Ghanbari (Representative)
Wood County Commissioners: Dr Theodore Bowlus; Doris Herringshaw; Craig LaHote
Secretary of State Frank LaRose

From: Coalition of Concerned Voters of Ohio

Subject: Security flaws in Dominion D-Suite voting machines used in Wood County may require the machines to be decertified.

Dear Board of Elections Directors and Board Members,

We are a coalition of voters in Ohio who are not affiliated with any political party, and like you, share the goal of ensuring that our election system in Ohio is secure, accurate, and can be trusted.

Over the past two and a half years, the Dominion ICX and D-Suite voting machines have been the subject of controversy and investigation with two independent teams of cybersecurity experts performing forensic examinations on Dominion machines in Georgia and Colorado. A Dominion ICX machine was examined in Fulton County Georgia and a D-Suite Election Management Server (EMS) machine was examined in Mesa County Colorado. The Georgia report is known as the Halderman Report and the Colorado report is divided into three volumes: Mesa County Colorado Reports 1, 2, and 3. Since these reports are lengthy, we have summarized their findings and provided links to the entire reports in the Appendix to this letter *"Summary of Dominion D-Suite Election Management System (EMS) and ImageCast X Voting System Security Flaws."*

Based on these extensive examinations, the voting machines were found to be unsafe for use in any election and, according to the well-credentialed experts who performed the forensic examination of the machines, should not have been certified in the first place. The Halderman report prompted CISA, the agency within the Department of Homeland Security (DHS) responsible for protecting our nation's election infrastructure, the issue a security advisory (ICSA-22-154-01) in June 2022 warning Board of Elections (BOE) of the security flaws. Additionally, the judge that presided over the lawsuit that produced the Halderman report felt that the merits of the case warranted it to go to trial beginning in January 2024.

It is sobering to note that both machines had been certified by a federally accredited Voting System Test Laboratory (VSTL) which means they met the specifications of a 2005 Voluntary Voting System Guideline (VVSG), developed primarily by the voting machine vendors

themselves. Apparently, the Georgia and Colorado machines were not examined and tested very well for security flaws and that, which is beyond the scope of this letter, raises questions about the certification process itself.

The Halderman Report revealed numerous security flaws that could be easily exploited by a malicious actor. For example, a QR barcode is printed on each ballot adjacent to the text that shows the voter's selections. The voter's selections are encoded into the QR code so that the machine can then read them, but the voter cannot. Halderman demonstrated how easy the QR code could be manipulated, therefore changing the vote. Since the voter cannot verify that the QR code accurately reflects the vote cast, this seems to be in violation of Ohio Revised Code (ORC) Chapter 3506.01 "Voting and tabulation equipment definitions," section (H) which states: *"After the physical paper printout is produced, but before the voter's ballot is recorded, the voter shall have an opportunity to accept or reject the contents of the printout as matching the voter's ballot choices."* It also appears to be a violation of the Help America Voting Act (HAVA) that requires voting machines to allow voters to verify ballots before they are cast.

The Mesa County reports show that critical files had been deleted and unauthorized software had been installed in the EMS causing a backdoor which allowed votes to be significantly altered.

These reports conclude that the machines are vulnerable to manipulation during an election and therefore raise the question that they may also be vulnerable to manipulation in support of an audit. Ohio performs post-election audits, which presumably gives a reasonable degree of confidence that the vote is accurate, and all twelve counties that use the Dominion machines employ a percentage-based audit whereby 5% of all ballots cast are audited. However, in an article *"How Ohio elections can SELECT rather than ELECT and escape post-election audit detection,"* one analyst presents a scenario whereby votes may be manipulated and not detected in the percentage-based audits that are used by the 12 counties that use the Dominion ICX machines. (See Reference 1 in the Summary Attachment).

Our concern is that the Dominion machines that are currently in use in Wood County and eleven other counties in Ohio, may also have similar security flaws that would render them unsafe for use in elections and may require them to be decertified. If so, we need to know what steps have been taken to mitigate or correct them. This is a serious matter, and the vendor (Dominion) cannot be relied upon to self-police themselves and point to a software patch as a fix. Since the VSTLs failed to catch these security flaws during certification, they cannot be relied upon either. Although the Ohio Bureau of Voting Machine Examiners (BVME) is responsible for examining and approving voting equipment for use in Ohio elections, they don't have the technical expertise either to adequately review the reports and perform the necessary cybersecurity forensic examinations of the Dominion voting machines in Ohio to determine their viability.

It is recommended that the Ohio Secretary of State appoint an independent team of cyber experts review the Halderman and Mesa County reports in their entirety and be given access to

the machines for examination to determine if security flaws exist. To protect any vendor proprietary information from being released, a non-disclosure agreement between the vendor and cyber team can be signed. Potential cyber expertise that the Secretary could enlist might include academia (Ohio colleges / universities with graduate computer science & engineering programs) or the Ohio Cyber Reserve (Oh CR) under the Command of the Adjutant General. Under their election security support mission, the Oh CR is authorized to assist local government entities (such as BOEs) at no cost with an independent team of cyber experts that can evaluate system security vulnerabilities and provide recommendations.

In closing, we request the following be provided to the undersigned by January 30, 2024:

1. Confirm that Wood County BOE has requested the Ohio Secretary of State to provide an independent team of cyber experts to review the Halderman and Mesa County Colorado reports and to examine the ICX and EMS machines in Wood County to determine their viability to be used in elections. If your decision is not to pursue this course of action, then provide your preferred alternate approach for ensuring that the machines are safe to be used in elections.

2. Describe the measures that Ohio BVME has taken to identify and disable any wireless modems embedded in the Dominion voting machines such as those reported in the Mesa County # 3 Report.

3. Dominion claims that a new software patch (Democracy Suite 5:17) has been released to address many of the security flaws. Confirm whether or not the new software has been installed and identify the specific security flaws in both the ICX and EMS machines that were addressed.

4. Does the EMS server contain unauthorized software (MS SQL Server Management Studio 17) as identified in the Mesa County Colorado #2 report?

5. According to the CISA advisory, the ImageCast X provides the configuration option to produce ballots that do not print barcodes (QR codes) for tabulation. Can you verify that this option applies to the Voter Verified Paper Audit Trail (VVPAT)? If so, how would that affect the audit?

Respectfully submitted,

Coalition of Concerned Voters of Ohio
PO Box 99, Dublin OH 43017
Email: CCVO@protonmail.com

Summary of
Dominion D-Suite Election Management System (EMS) and
Imagecast X (ICX) Voting System Security Flaws
(Halderman and Mesa County Colorado Reports)

Overview

The security and trustworthiness of our voting machines and our voting system at large is paramount to keeping and maintaining our democracy. Unfortunately, the atmosphere surrounding elections has become so politicized over the past few years that it has stifled honest and open discussion when it comes to concerns about the integrity of our voting machines.

As you are aware, concerns over electronic voting machines are not new and span over twenty years. After Kerry's loss to Bush in 2004, Hillary Clinton's loss to Trump in 2016, and more recently with Trump's loss to Biden in 2020, the integrity of electronic voting machines has been called into question and valid questions have been raised. Specifically, in the aftermath of the 2004 and 2016 presidential elections, multiple investigations and Congressional hearings were held and expert witnesses under oath concluded that electronic voting machines can be easily hacked and programmed to alter elections.

In 2018, county election boards across Ohio went through the process of choosing new vendors to replace outdated voting machines. At the time, some counties were using Direct Recording Electronic (DRE) touchscreen machines without paper ballots that recorded voter's selections in the internal memory of the voting machine. After a number of cyber experts warned that the DRE machines were vulnerable to manipulation, many counties decided to switch to paper ballots that could be optically scanned. It is our understanding that twelve counties in Ohio including Adams, Butler, Fairfield, Greene, Hancock, Harden, Madison, Perry, Richland, Scioto, Stark and Wood, chose the Dominion ICX and D-Suite EMS Direct Recoding Electronic (DRE) system with voter verified paper audit trail.

The Halderman Report

Link to Report: The redacted version of the *"Security Analysis of Georgia's ImageCast X Ballot Marking Devices"* aka The Halderman Report, can be accessed at https://storage.courtlistener.com/recap/gov.uscourts.gand.240678/gov.uscourts.gand.240678.1681.0.pdf

Background

The forensic examination of the Dominion machines in Georgia had its origins in a lawsuit (Curing v. Raffensperger) filed in 2017 by voters in Georgia who suspected that their aging ES&S Direct Recording Electronic (DRE) voting machines purchased in 2005 were not trustworthy and needed to be replaced. The ES&S machines did not have a paper ballot and stored voters cast in its internal memory. The Secretary of State opted to replace the ES&S machines with the Dominion ImageCast X Ballot Marking Device system, which is also a DRE voting machine, but prints out a ballot with the voter's selection in text and a QR barcode that encodes the vote so that it can be read by an optical scanner. However, after experiencing issues with the Dominion machines in the 2018 midterm election, the original plaintiffs continued with their lawsuit stating that the Dominion machines could not be trusted.

In September 2020, the plaintiff's hired a renowned cybersecurity expert to perform a six-week forensic examination on one of the machines and they discovered vulnerabilities in nearly every part of the system that is exposed to potential attackers. The findings were sobering and substantial enough to prompt a nation-wide security advisory to be issued to all BOEs by CISA, the agency within the Department of Homeland Security charged with protecting the nation's election system.

Initially, the Halderman report was sealed by court order for two years over concerns that revelations of the security flaws could be capitalized on by malicious actors. A redacted version was eventually released to the public in June 2023. Given the gravity of the situation, the Judge that presided over the original lawsuit released an opinion on 10 November 2023 that the case needed to go to trial to determine whether Georgia's statewide electronic voting system, as currently designed and implemented, suffers from major cybersecurity deficiencies that would allow votes to not be counted accurately. The trial is scheduled to begin in January 2024.

Halderman Report Findings

The Halderman report findings were significant enough to prompt CISA, the agency under the Department of Homeland Security responsible for protecting our election infrastructure, to release a security advisory (ICSA-22-154-01) in June 2022 warning BOEs about the ICX machine security flaws and that the security risks should be mitigated as soon as possible. However, unlike the Halderman Report, CISA's advisory contained few details about the problems identified, therefore downplaying the scope and depth of the findings in the actual report.

Although CISA's security advisory contained the caveat "*While these vulnerabilities present risks that should be promptly mitigated, CISA has no evidence that these vulnerabilities have been exploited in any election,*" it could also be said that CISA has no evidence that the vulnerabilities have not been exploited. Case in point,

CISA's highly classified network was hacked in 2020 by a cyberattack known as Solar Winds (see Reference 2 in the Summary Attachment). As bad as it was for the agency charged with protecting our nation's election system to be hacked, what made it worse was that it went undetected for a year and CISA still does not know the extent of the data that was compromised. If CISA was unaware of its own network being hacked, it doesn't instill confidence when they say they have no evidence that the Dominion machines have been hacked. It is entirely possible that the machines have been and continue to be exploited without being detected.

The Halderman Report's major finding was that the QR codes printed on the BMD ballots and DRE paper audit trail can be altered without the voter's knowledge through a simple hack of the ICX machine itself, or more likely from an arbitrary-code-execution vulnerability that can be exploited to spread malware from the county's central election management system (EMS) to every BMD / DRE in the jurisdiction. This makes it possible to attack the ICX BMDs / DREs at scale, over a wide area, without needing physical access to any of them.

It is important to note that the Georgia ICX BMD machines are identical to the ICX Direct Recording Electronic (DRE) machines used in Ohio with the exception that the BMD prints voter selections onto a ballot whereas the DRE machines print voter selections onto a voter-verified paper audit trail (VVPAT) tape that is enclosed in the machine. In both cases, voter selections are converted into a QR code that is printed on the ballot / VVPAT tape that is then read by the machine to tally the votes. The problem is that the voter has no way of verifying that the QR code has accurately captured the vote since they can't read it. This flaw was first identified by a Democrat-led Congressional Task Force on Election Security in 2018 (See Reference 3 below):

> *"Some DRE machines have a VVPAT that allows voters the opportunity to review a printout of their selections before casting a ballot. However, the VVPAT system has two flaws. First, voters are unlikely to actually review the paper record to make sure it is accurate. Second, votes are still recorded on the internal memory of the machine.* ***That means a hacker could infect the machine in a way where the paper printout reflects the voter's actual preference, but the machine's internal memory records a different vote.*** *In other words, the printout does not necessarily verify whether the machine is tabulating correctly. Moreover, in the process of implementing risk-limiting audits, Colorado has found that VVPAT systems create significant logistical hurdles and are much harder to audit than paper ballots. As a result, several experts we spoke to believe that the VVPAT machines should be phased out as well."*

Following the release of the Halderman Report, Dominion produced a new software version, Democracy Suite 5.17 that purportedly addresses several of the vulnerabilities described in the report. The patched software entered federal certification testing in October 2022 and was certified by the U.S. Election Assistance Commission in March

2023. Halderman was not given access to the updated software (nor to his knowledge neither has CISA been given access) so he cannot verify whether the changes are effective. It has been reported that the Ohio BVME has informed at least one of the twelve affected Ohio County BOEs (Butler) of Dominion's software patch to correct the security flaws. However, according to a recent CNN news article (see Reference 6 below), Georgia election officials say that upgrading the ICX machines would be such a massive undertaking that they have decided to wait until after the 2024 election to do so. The bottom line is that the version 5.17 software patch appears to be a large update and may not address all of the CISA advisory security flaws. In addition, it is not clear whether it addresses the EMS security flaws discovered in the Mesa County reports.

The MITRE Report

As a rebuttal to the Halderman Report, Dominion hired The MITRE Corporation to do an "Independent Technical Review" of the Georgia ICX machines. The report concluded that Halderman's attacks were "operationally infeasible" due to the physical controls in place in the state and the low likelihood of flipping enough votes to make an impact. Access to the report can be found at this link: https://sos.ga.gov/sites/default/files/2023-06/MITRE%20Report.pdf.

Based on the findings of the MITRE Report, Georgia's Secretary of State Raffensperger defended the Dominion ICX machines in a letter (see Reference 4 below) to the Georgia state General Assembly in June 2023. The following is an excerpt of his remarks:

"The Halderman report was the result of a computer scientist having complete access to the Dominion equipment and software for three months in a laboratory environment. It identified risks that are theoretical and imaginary. We have to run elections in the real-world, not just create conspiracies or hypothetical possibilities. Our security measures are real and mitigate all of them."

The day the Halderman Report was released to the public, Halderman challenged the findings of the MITRE Report in a news article published in June 2023 (see Reference 5 below) by stating:

"In March 2022, Dominion hired MITRE to respond to my Report. Unlike me and my assistant, Dominion did not give MITRE access to the voting equipment or software, so they couldn't perform any actual security tests. Instead, MITRE assessed the attacks described in our report without essential access to the source information.....MITRE's analysis, which is unsigned, applies faulty reasoning to assert that exploiting the vulnerabilities is 'operationally infeasible." This contradicts CISA's determination that "these vulnerabilities present risks that should be mitigated as soon as possible."

MITRE's analysis isn't simply wrong—it is dangerous, since it will surely lead states like Georgia to postpone installing Dominion's software updates and implementing other important mitigations. Considering the overwhelming evidence of physical security lapses in Georgia and other states, MITRE should retract the report, which fails to account for the real-world conditions under which election equipment is stored and operated. More than 25 leading experts in cybersecurity and election security have sent a letter to MITRE CEO Jason Providakes urging him to retract MITRE's dangerously mistaken report."

The Mesa County Colorado Reports

Background

The Mesa County Colorado reports were initiated by the Mesa County Colorado Clerk / Recorder Tina Peters who turned whistleblower after discovering that her Secretary of State wanted to do a major update to the voting machines after the 2020 election without first making backups. She was concerned that if she allowed updates to be made without a backup, she would be in violation of federal law that mandates the preservation of election data. She then made backups prior to and after the 2020 general election and the following 2021 primary election and hired an expert cybersecurity team to preserve data and determine if there were any changes made because of the updates. The examination occurred over a six-month period from September 2021 to March 2022 at the Mesa County Colorado BOE and resulted in the release of three reports.

When CISA issued their security advisory in response to the Halderman Report, they provided a caveat that "no evidence has been brought forth to show that the ICX system vulnerabilities have altered any elections." However, the advisory did not address the Election Management System (EMS) server. The Mesa County Colorado Reports looked at the EMS server in Mesa County and provided convincing evidence that the Dominion EMS server they examined altered the outcomes of the 2020 and 2021 elections in Mesa County Colorado. To date, CISA has not acknowledged the findings of the Mesa County Reports and the findings of the Mesa Reports were disputed by the Mesa County District Attorney (DA), who launched a criminal investigation after the reports were published. Although the DA concluded that the problems identified in the Mesa Reports were attributed to human error, the authors of the Mesa reports countered by noting that the DA did not use an independent cybersecurity expert to review their findings and could not name a single conclusion in the report that was false, much less provide any evidence that a conclusion was false.

Findings

The findings of the Mesa County Reports are even more incriminating than those of the Halderman Report and provide alarming and conclusive evidence that the Mesa County Dominion D-Suite EMS server contained unauthorized software and was purposely programmed to manipulate votes.

Mesa County Report # 1 Findings
Title: Forensic Examination and Analysis Report (69 pages)
Issued: September 15, 2021; Author: Doug Gould
Link to report: https://static1.squarespace.com/static/620c3af99f21b965e2cbef44/t/622638ae2bbc6b1e5e988cf3/1646672059000/Mesa-EMS-Server-Image-Forensic-Report-No-1-09-15-21.pdf

"Analysis of the Mesa County EMS server identified that extensive deletion of both election data and election-related data, comprising election records which must and should have been preserved under Federal and Colorado law, has occurred either because of or coincident with the vendor's and CO Secretary of State's modification of the system from version 5.11 to 5.13. This deleted data is critical to any effort to reconstruct events taking place on the voting systems, and to determine of unauthorized access or operation of the voting system took place."

Mesa County Report # 2 Findings
Title: Forensic Examination and Analysis Report (136 pages)
Issued: February 28, 2022; Author: Doug Gould
Link to report: https://static1.squarespace.com/static/620c3af99f21b965e2cbef44/t/62268289a0e00c56951c5044/1646690974087/mesa-county-forensic-report-no.-2+compressed+1.1.pdf

- *"Based on testing, the Election Management System (EMS) server is not secure and violates security standards required by state and federal law and protections have not been implemented in accordance with the requirements of the Federal Election Commission's 2002 Voting System Standards (VSS). Those Standards constitute a mandatory minimum requirement for a voting system to be certified and used under Colorado law.* ***Given the fundamental flaws in the security design and configuration of this system, there is no conceivable interpretation under which this voting system could be considered secure.*** *The fact that it was tested and certified for use vitiates claims of competency and trustworthiness of the entire regime of testing and certification being used, of truthfulness of testing and certification statements, of competency of the Colorado Secretary of State's office, and of the validity of any election results obtained from the voting system as used in any jurisdiction."*

- *"Uncertified software (MS SQL Server Management Studio 17) was installed that violates and renders illegal the certification of the election system to be used in an election. As configured, it creates a 'back door' that allows the bypassing of Dominion Voting System's software and enables any data in the vote data base to be changed. In other words, votes can be flipped and by changing only two values in the database, tens of thousands of votes can be flipped."*

- *"Mandatory audit trails (logs) had been deleted making it extraordinarily difficult (and maybe impossible) to forensically determine whether any external connection allowing unauthorized access to the voting system, wireless or wired, occurred before, during or after the elections."*

- *"The Mesa County EMS server used through May 2021 was assembled in Mexico, and its motherboard was manufactured in China. It is well understood that foreign manufacture or assembly exposes the components to the risk of compromise through the installation of foreign-controlled access devices during manufacture in the reported supply-chain attack."*

Mesa County Report # 3 Findings
Title: Election Database and Data Process Analysis (68 pages)
Issued: March 10, 2022; Authors: Jeffrey O'Donnell & Walter C. Daugherty.
Link to report: https://static1.squarespace.com/static/620c3af99f21b965e2cbef44/t/6239f21179bda53621a515e2/1647964693221/mesa-forensic-report-3-signed+%281%29.pdf

This report documents the findings of an examination of tabulated vote databases based on forensic analysis of the drive image of Mesa County, Colorado's Dominion Voting Systems (DVS) Election Management System (EMS) server. This analysis was performed using the forensic image of the EMS server, which was backed up before Colorado Secretary of State and DVS overwrote the hard drive with D-Suite version 5.13.

- *"There were unauthorized creations of new tabulation and adjudication databases on the election management server during the November 2020 General Election and 2021 Municipal Election along with selective copying of batch and ballot records from the original databases to the new ones.* ***This manipulation places all initial ballots counted into a state where they cannot be validated, therefore the system cannot be considered reliable to be used in any election."***

- *"The ballot record manipulation described above would not be identifiable to an election official using the voting systems, nor to an observer or judge overseeing*

the election conduct, much less to citizens with no access to the voting systems; without both cyber and database management system expertise, and unfettered access to database records and computer log files (many of which were destroyed by the actions of the Secretary of State) from the EMS server, the manipulation would be undetectable."

- *"Multiple wireless access devices are known to be embedded in the Dominion Voting System (DVS) hardware (36 were found to exist in DVS-D suite components as documented by Dell and the equipment inventory list). The forensic team used a wireless modem to emulate those found in the machines and given the insecure configuration of the server, they were able to edit and change vote totals using a standard I Phone!"*

Mesa County Colorado District Attorney (DA) Challenge to Mesa County Report # 3

In May 2022, soon after the Mesa # 3 report was released, The Mesa County DA's office launched a criminal investigation into the serious allegations raised in the Mesa # 3 report. The DA's conclusion (see Reference 7 below) was that the key issue raised by the Mesa #3 report (i.e. the creation of an unauthorized database) was caused by human error, and not by malicious software in the Dominion voting machine. This investigation was closed with no finding of probable cause that a crime was committed by any person.

Mesa Report # 3 Author's Rebuttal to the Mesa DA Criminal Investigation

The cybersecurity experts who authored the Mesa # 3 report released an official response in May 2022 (see Reference 8 below) to the conclusions reached by the Mesa County DA's investigation. The following are excerpts from their response:

- *"The DA Report did not name a single conclusion in the report that was false, much less provide ANY evidence that a conclusion was false. In the third Mesa Forensic Report, the authors list three possible causes of the anomalies and give their expert opinions that on-site human action was the least likely based on interviews with those involved. The DA claims to have proven that it was on-site human action which caused the anomalies without ever looking the databases involved or engaging an independent expert to do so, given that the investigators have no database expertise."*

- *"The DA's office discussed a possible method by which the new database could have been created, should a clerk perform a highly unusual procedure which is extremely dangerous when done in the middle of tabulating an election. The video presented as "evidence" shows absolutely no definitive screen detail to support the DA's claims that this "nuclear option" was ever performed. In addition, the EMS logs, which show in great detail the operations performed by both the clerks*

and the normal automated processes within the Dominion software application, show no corresponding commands being initiated. This fact alone is evidence that the unauthorized operations were triggered by code running within the EMS server but outside of normal procedure. "

- *"Additionally, did the DA's office or any of their technical experts access the publicly available forensic image of the Mesa County server taken before representatives of the Colorado Secretary of State and Dominion Voting Systems erased all files on that server? If not, how can the DA plausibly investigate the findings and conclusions of Report #3, which were completely derived from that forensic image?"*

- *"In summary, the DA's report is lacking any evidence to refute any of the findings or conclusions of Report #3, and we find that the DA's report is completely lacking any evidence or technical rigor of a serious, unbiased investigation."*

References:

1. ***How Ohio elections can SELECT rather than ELECT and escape post-election audit detection***. Link: https://www.ohio4truth.com/post/how-ohio-elections-can-change-from-elected-to-selected-and-escape-post-election-audit-detection

2. **April 16, 2021 *NPR* article: "A 'Worst Nightmare' Cyberattack: The Untold Story of the Solar Winds Hack".** Link: https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

3. ***2018 Congressional Task Force on Election Security* (p.24 under "Findings)."**

   https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjl7v6G2aiDAxUZg4kEHaZmCmIQFnoECA8QAQ&url=https%3A%2F%2Fwww.hsdl.org%2Fc%2Fview%3Fdocid%3D808309&usg=AOvVaw3AQ_bCtOx9INoDy6xLSXEQ&opi=89978449

4. **June 20, 2023 Letter from Georgia Secretary of State to GA General Assembly:" Setting *the Election Security Record Straight*" Link: https://sos.ga.gov/news/setting-election-security-record-straight**

5. **June 14, 2023 article published on *Freedom-to-Tinker.com* website "*Security Analysis of the Dominion ImageCast X*" by J. Alex Halderman Link: https://freedom-to-tinker.com/2023/06/14/security-analysis-of-the-dominion-imagecast-x/**

6. June 14, 2023 *CNN* News article "Georgia won't update vulnerable Dominion software until after 2024 election." Link: (https://www.cnn.com/2023/06/14/politics/dominion-voting-georgia-vulnerabilities-2024/index.html)

7. May 19, 2022 letter "Conclusion of investigation of Report 3 re: Elections." from Daniel P. Rubenstein, District Attorney to Mesa County Commissioners and Grand Junction City Council. Link: https://wp-cpr.s3.amazonaws.com/uploads/2022/05/Summary-of-findings-and-conclusions-of-Report-3.pdf

8. Official Response to Mesa DA Investigation. Fact check of Rubebstein's Investigative Report by Randy Corporon, Attorney for Tina Peters. Link: https://tinapeters.us/wp-content/uploads/2023/11/OFFICIAL-STATEMENT-5-20.pd